Universidad de El Salvador. 6.12.2018
Álgebra II. Examen parcial 2. Soluciones

Problema 1 (2 puntos)**.** Para el polinomio $f := X^3 + 3X + 2 \in \mathbb{Q}[X]$, sean K el anillo cociente $\mathbb{Q}[X]/(f)$ y $\alpha \in K$ la imagen de X en el cociente.

a) Demuestre que K es un cuerpo. [$\frac{1}{2}$ *punto*]

b) Exprese α^{-1} en la base $1, \alpha, \alpha^2$. [$\frac{1}{2}$ *punto*]

c) ¿Es cierto o falso que existe $\beta \in K$ tal que $\beta^3 = \alpha$? [1 *punto*]

Solución. En a), sabemos que K es un cuerpo si y solo si f es irreducible en $K[X]$. El polinomio es cúbico, así que f es irreducible si y solamente si f no tiene raíces en K. Según el teorema de las raíces racionales, las posibles raíces son ± 1 y ± 2, pero se tiene

$$f(1) \neq 0, \quad f(2) \neq 0, \quad f(-1) = -2 \neq 0, \quad f(-2) = -12 \neq 0.$$

De otra manera, se podía observar que $f(X+1) = X^3 + 3X^2 + 6X + 6$ es irreducible por el criterio de Eisenstein para $p = 3$, así que f es también irreducible.

En b), si $\alpha^{-1} = a\,\alpha^2 + b\,\alpha + c$, entonces tenemos

$$1 = \alpha\,\alpha^{-1} = a\,\alpha^3 + b\,\alpha^2 + c\,\alpha = a\,(-3\alpha - 2) + b\,\alpha^2 + c\,\alpha = b\,\alpha^2 + (c - 3a)\,\alpha - 2a,$$

de donde $a = -\frac{1}{2}$, $c = -\frac{3}{2}$, $b = 0$, así que $\alpha^{-1} = -\frac{1}{2}\,\alpha^2 - \frac{3}{2}$.

El polinomio mínimo de α sobre $\mathbb{Q}$ es $X^3 + 3X + 2$ y este coincide con el polinomio característico, de donde $N_{K/\mathbb{Q}}(\alpha) = -2$. Si $\beta^3 = \alpha$, entonces $N_{K/\mathbb{Q}}(\beta)^3 = N_{K/\mathbb{Q}}(\alpha)$, pero esto es imposible ($\sqrt[3]{-2} \notin \mathbb{Q}$). Entonces, la respuesta a la pregunta de c) es negativa. ■

Problema 2 (2 puntos)**.** Sean p un número primo y $n = 1, 2, 3, \ldots$ Para el cuerpo finito $\mathbb{F}_{p^n}$ y un elemento $\alpha \in \mathbb{F}_{p^n}$ definamos $t(\alpha) := \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$.

a) Demuestre que $t(\alpha) \in \mathbb{F}_p$. [1 *punto*]

b) Demuestre que $t\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ es una aplicación $\mathbb{F}_p$-lineal. [$\frac{1}{2}$ *punto*]

c) Demuestre que la aplicación $t\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ es sobreyectiva. [$\frac{1}{2}$ *punto*]

Solución. Tenemos $x \in \mathbb{F}_p$ si y solo si $x^p = x$. En nuestro caso,

$$t(\alpha)^p = \left(\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}\right)^p = \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^n} = t(\alpha)$$

— esto está claro si $\alpha = 0$, y si $\alpha \neq 0$, observamos que $\alpha^{p^n} = \alpha^{p^n - 1}\,\alpha = \alpha$ porque el grupo $\mathbb{F}_{p^n}^\times$ tiene orden $p^n - 1$.

Para la parte b), basta recordar (o verificar otra vez más) que el automorfismo de Frobenius $F\colon x \mapsto x^p$ es una aplicación $\mathbb{F}_p$-lineal (esto se sigue del teorema del binomio en característica p y el pequeño teorema de Fermat) y tenemos

$$t(\alpha) = \alpha + F(\alpha) + F^2(\alpha) + \cdots + F^{n-1}(\alpha).$$

En la parte c), ya que tenemos una aplicación $\mathbb{F}_p$-lineal con valores en $\mathbb{F}_p$, bastaría probar que $\operatorname{im} t \neq 0$. En efecto, la ecuación polinomial

$$t(X) = X + X^p + \cdots + X^{p^{n-1}} = 0$$

no puede tener más de p^{n-1} raíces, así que existe[*] $\alpha \in \mathbb{F}_{p^n}$ tal que $t(\alpha) \neq 0$. ■

[*] En general, *no está claro* para cuáles $\alpha \in \mathbb{F}_{p^n}$ se tiene $t(\alpha) \neq 0$. Por ejemplo, si $\alpha \in \mathbb{F}_p$, entonces $t(\alpha) = \alpha + \alpha + \cdots + \alpha = n\alpha$, pero si $p \mid n$, este elemento es nulo.

Problema 3 (2 puntos)**.** Sea p un número primo. Consideremos el polinomio $f := X^2 + X + 1 \in \mathbb{F}_p[X]$.

a) Demuestre que f es irreducible si y solo si $p \equiv 2 \pmod 3$. [1 *punto*]

b) ¿Para cuáles p el polinomio f es separable? [1 *punto*]

Primera solucion. Si $p = 2$, este polinomio es irreducible. Si $p \neq 2$, sus raíces en un cuerpo de descomposición vienen dadas por

$$\frac{-1 \pm \sqrt{-3}}{2}.$$

Estos elementos pertenecen a $\mathbb{F}_p$ si y solo si $\sqrt{-3} \in \mathbb{F}_p$. Entonces, el polinomio es irreducible si y solo si

$$\left(\frac{-3}{p}\right) = -1.$$

Para $p \neq 3$ calculamos usando la ley de reciprocidad cuadrática

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Los cuadrados módulo 3 son 0 y 1, así que para $p \neq 3$

$$f \text{ es irreducible} \iff \left(\frac{p}{3}\right) = -1 \iff p \equiv 2 \pmod 3.$$

Para $p = 3$ el polinomio $X^2 + X + 1 = (X-1)^2$ es reducible.

Para $p = 2$ el polinomio es separable: en efecto, en este caso es irreducible y $f' = 2X + 1 = 1 \neq 0$. Si $p \neq 2$, el polinomio *no es* separable precisamente cuando sus dos raíces en un cuerpo de descomposición coinciden:

$$\frac{-1+\sqrt{-3}}{2} = \frac{-1-\sqrt{-3}}{2} \iff +\sqrt{-3} = -\sqrt{-3} \iff \sqrt{-3} = 0 \iff p = 3.$$

Conclusión: el polinomio es separable para cualquier p excepto $p = 3$. ■

Segunda solución (Moisés Daniel). El polinomio $f := X^2 + X + 1$ es el tercer polinomio ciclotómico. Tenemos

$$X^3 - 1 = f\,(X-1).$$

Notamos que $f(1) = 3$, así que 1 es una raíz de f si y solo si $p = 3$.

Asumamos ahora que $p \neq 3$. En este caso las siguientes condiciones son equivalentes:

1) f es reducible;

2) f tiene una raíz en $\mathbb{F}_p$;

3) en $\mathbb{F}_p^\times$ hay un elemento de orden 3;

4) $3 \mid (p-1) \iff p \equiv 1 \pmod 3$.

En efecto, 1) y 2) son equivalentes porque f tiene grado 2. Además, 3) y 4) son equivalentes porque el grupo $\mathbb{F}_p^\times$ es cíclico de orden $p-1$.

Asumamos que se cumple 2). Si $a \in \mathbb{F}_p$ es una raíz de f, entonces a es una raíz de $X^3 - 1$. Tenemos necesariamente $a \neq 0, 1$, así que a es un elemento de orden 3 en $\mathbb{F}_p^\times$. Esto establece 3).

Viceversa, la condición 3) es equivalente a existencia de $a \in \mathbb{F}_p^\times$ tal que $a \neq 1$ y $a^3 = 1$. Analizando la identidad $X^3 - 1 = f(X-1)$, se ve que esto es equivalente a $f(a) = 0$. Entonces, 3) implica 2).

Estas consideraciones nos permiten concluir que f es *reducible* si y solamente si $p = 3$ o $p \equiv 1 \pmod 3$. En otras palabras, f es *irreducible* si y solamente si $p \equiv 2 \pmod 3$. Esto demuestra la parte a).

En la parte b) bastaría notar que el polinomio $X^3 - 1$ es separable si y solamente si $p \neq 3$ (véase el problema 4), y entonces $X^2 + X + 1$, siendo su factor, es separable para todo $p \neq 3$. ■

Problema 4 (2 puntos)**.** Sean p un primo impar y n un número natural tal que $p \nmid n$. Denotemos por $\Phi_n \in \mathbb{Z}[X]$ el n-ésimo polinomio ciclotómico.

a) Demuestre que el polinomio $X^n - 1 \in \mathbb{F}_p[X]$ es separable. [1 *punto*]

b) Demuestre que si $a \in \mathbb{Z}$ satisface $\Phi_n(a) \equiv 0 \pmod p$, entonces $p \nmid a$ y el orden de a en $(\mathbb{Z}/p\mathbb{Z})^\times$ es igual a n. [1 *punto*]

Indicación: factorice $X^n - 1 \in \mathbb{Z}[X]$ en polinomios ciclotómicos.

Solución. De hecho, la parte a) fue probada en clase. Basta calcular que para $f = X^n - 1$ se tiene $f' = nX^{n-1}$. Por nuestra hipótesis tenemos $n \neq 0$ en $\mathbb{F}_p$ y luego $\operatorname{mcd}(f, f') = 1$[*].

En la parte b), escribamos

$$X^n - 1 = \Phi_n \cdot \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d.$$

Si $\Phi_n(a) \equiv 0 \pmod p$, entonces $a^n \equiv 1 \pmod p$, y en particular $p \nmid a$. Para ver que el orden de a es precisamente n, basta notar que si $a^d \equiv 1 \pmod p$ para $d < n$, entonces la ecuación de arriba implica que a es una raíz múltiple de $X^n - 1$ en $\mathbb{F}_p$, pero no es el caso según lo que probamos en a).

He aquí un ejemplo: el polinomio ciclotómico $\Phi_3 = X^2 + X + 1$ tiene raíces 2 y 4 módulo 7 y los órdenes de 2 y 4 módulo 7 son iguales a 3. ■

Problema 5 (2 puntos)**.** Sean p un número primo y $a \in \mathbb{F}_p$ un elemento no nulo. Consideremos el polinomio $f := X^p - X + a \in \mathbb{F}_p[X]$. En este problema vamos a probar que f es irreducible.

a) Demuestre que f es separable. [$\frac{1}{2}$ *punto*]

b) Sea L un cuerpo de descomposición de f y sea $\alpha \in L$ un elemento tal que $f(\alpha) = 0$. Demuestre que las raíces de f en L son $\alpha, \alpha + 1, \ldots, \alpha + p - 1$. [$\frac{1}{2}$ *punto*]

c) Asumamos que $f = gh$ donde $g, h \in \mathbb{F}_p[X]$ son polinomios mónicos y $\deg g, \deg h < \deg f$. Analizando la suma de las raíces de g o h, concluya que $\alpha \in \mathbb{F}_p$. [$\frac{1}{2}$ *punto*]

d) Demuestre que en este caso f se descompone en factores lineales en $\mathbb{F}_p[X]$ y deduzca una contradicción. [$\frac{1}{2}$ *punto*]

Solución. En a) basta calcular que $f' = pX^{p-1} - 1 = -1$, así que $\operatorname{mcd}(f, f') = 1$.

En b), notamos que si $f(\alpha) = 0$, entonces

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) + a = \alpha^p + i - (\alpha + i) + a = f(\alpha) = 0.$$

Esto demuestra que $\alpha + i$ es una raíz de f para cualquier $i = 0, 1, \ldots, p - 1$. En un cuerpo de característica p todos estos p elementos son diferentes y sabemos que f tiene p raíces en L, así que estas son todas las raíces de f.

[*] Algunos dijeron que $X^n - 1$ es separable porque sus raíces complejas son las n-ésimas raíces de la unidad $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$, pero esto demuestra la separabilidad en $\mathbb{Q}[X]$ y no en $\mathbb{F}_p[X]$.

En c), notamos que en $L[X]$ tenemos

$$g = (X - (\alpha + i_1)) \cdots (X - (\alpha + i_k)) = X^k - (k\alpha + (i_1 + \cdots + i_k))\, X^{k-1} + \cdots,$$

donde $0 < k < p$. Además, $g \in \mathbb{F}_p[X]$, así que

$$k\alpha + (i_1 + \cdots + i_k) \in \mathbb{F}_p.$$

Puesto que $k \neq 0$ en $\mathbb{F}_p$, esto demuestra que $\alpha \in \mathbb{F}_p$.

En fin, lo que probamos en c) nos dice que $\alpha + i \in \mathbb{F}_p$ para $i = 0, \ldots, p-1$ son las raíces de f. Pero estos son precisamente todos los elementos de $\mathbb{F}_p$. Sin embargo, $f(0) = a \neq 0$ por nuestra hipótesis. Esto establece la parte d). ■